Module 5

DOE Standard 1189

September 29, 2009 **3:00 – 5:00**

NUCLEAR EXECUTIVE
LEADERSHIP TRAINING

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Integrating Safety into the Design Process

Jim O'Brien
Office of Nuclear Safety Policy and Assistance, HSS

Dr. O'Brien is the Director of the Office of Nuclear Safety Policy and Assistance (HS-21) within the Office of Health Safety and Security. In this role Dr. O'Brien develops and maintains the Department of Energy (DOE) nuclear safety Directives and Standards and provides assistance to DOE Program and Field Offices in implementing the nuclear safety requirements and sharing best practices.

Dr. O'Brien has over 25 years experience in nuclear engineering, operations, and safety. He has 10 years experience at a shift supervisor, reactor engineer, and project engineer at a commercial nuclear power plant. He has 9 years experience at the Nuclear Regulatory Commission where he participated in the development of nuclear safety requirements and standards related to renewing commercial nuclear power plant licenses and emergency preparedness. He has 5 years experience in the oversight of DOE's emergency management and nuclear safety programs and their implementation. The last three years he has been Director of HS-21, and been leading the completion of a Nuclear Material Packaging Manual, the revision of DOE's Standard on hazard Categorization (DOE-STD-1027), and the resolution of several Defense Nuclear Facilities Safety Board Recommendations and issues.

Dr. O'Brien's Office developed, with the critical support of DOE Program Offices and the Energy Facility Working Group, DOE Standard 1189, *Integrating Safety into the Design Process*, recently completed and conducted a Pilot Course to support its implementation, and is currently updating several DOE Directives and Standards to conform with new safety design processes and criteria specified in DOE Standard 1189..

Dr O'Brien holds a bachelor's degree in nuclear engineering from North Carolina State University, a master's degree in materials engineering from Drexel University, and a PhD in nuclear engineering from the University of Maryland. He is a registered Professional Engineer.

Jim McConnell
Office of Safety, NNSA

Mr. McConnell is the Director of the Office of Safety within NNSA Defense Programs. In this role Mr. McConnell provides direct management support to senior leaders in Defense Programs for all nuclear safety and non-nuclear safety functions and issues. The scope of safety functions

includes executing the NNSA self-regulatory requirements for nuclear safety and worker safety within Defense Programs.

As the Chief of Defense Nuclear Safety in the National Nuclear Security Administration (NNSA), Mr. McConnell was responsible for the development and implementation of NNSA-wide safety programs. His role was to increase corporate focus on nuclear safety and to coordinate safety issues at the NNSA site offices and headquarters. He reported directly to the NNSA administrator and advised NNSA on its interactions with the DOE, DNFSB, and other federal, state, and local agencies on matters relating to nuclear safety.

Mr. McConnell has spent a majority of his career in the oversight of nuclear safety. Spending 12 years at the DNFSB, he most recently was deputy technical director. In that position, he directed the board's technical staff and provided overall strategic planning to achieve the board's technical safety oversight mission. In this capacity, Mr. McConnell also served on the INPO Advisory Panel for Nuclear Safety Culture. During his tenure at DNFSB, he served as a group leader of the Nuclear Weapons Program, a site representative at the Pantex Plant, program manager for the Y-12 National Security Complex at Oak Ridge and a technical specialist. A former U.S. Navy officer, he served on the USS Houston and was an instructor at the SIC Nuclear Prototype Training Unit in Windsor, Connecticut.

He holds a bachelor's degree in electrical engineering from the U.S. Naval Academy and masters' degrees from the Catholic University of America and George Washington University.

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Integration of Safety into the Design Process

Jim O'Brien, Director,
Office of Nuclear Safety Policy and Assistance, HSS
and
Jim McConnell, Director,
Office of Safety, NNSA

Learning Objectives

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

At the end of this module, students should know:

- DOE's expectations for integrating safety into design
- The Standard 1189 key concepts and guiding principles, and the important processes and documents which support integrating safety into design
- Line management's responsibilities for integrating safety into design
- The importance of ensuring early integration of safety into design

Deputy Secretary Expectations

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

I expect safety to be fully integrated into design early in the project. Specifically, by the start of the preliminary design, I expect a hazard analysis of alternatives to be complete and the safety requirements for the design to be established. I expect both project management and safety directives to lead projects on the right path so that safety issues are identified and addressed adequately early in the project design.

– Deputy Secretary of Energy, December 5, 2005

Deputy Secretary Expectations (Continued)

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

- I expect line project teams to have the necessary experience, expertise, and training in design engineering, safety analysis, construction, and testing.
- I expect that the Chiefs of Nuclear Safety will provide safety oversight during the design, construction, and testing phases of our projects.
- I expect staff work and presentations to the ESAAB to be sufficiently complete so that they highlight tailoring issues and safety issues that need management attention.
- I expect that we will learn effectively from our project experience so that future projects are more likely to be completed on time and on budget with all mission and safety objectives satisfied.

Introduction to DOE-STD-1189
Integration of Safety into the Design Process

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

The Standard addresses the first of the Deputy Secretary's expectations: "I expect safety to be fully integrated into design early in the project."

Standard 1189:

- Shows how project management, design, and safety can work together to integrate safety into design
- Describes the process for effective interactions of the various project organizations- management, engineering design, safety analysis, and final authorization to operate
- Defines format and content of safety design basis documents at each design stage
- Includes objective criteria for classification of safety SSCs and seismic classification of SSCs

GUIDING PRINCIPLES

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Derived from DOE O 420.1B, DOE O 413.3A, and associated Guides

1. Use of O 420.1B and clearly articulated strategies to satisfy requirements
2. Control selection strategy order of preference
3. Following design codes and standards in O 420 guides
4. Use of risk and opportunities assessments
5. Conservative early project safety decisions input to cost/schedule
6. CD packages portray safety decisions
7. Project team includes appropriate expertise
8. Safety personnel involved from onset of project planning
9. Important safety functions addressed during conceptual design
10. Safety Design Integrating Team (SDIT) invokes the STD-1189 process
11. All stakeholder issues identified early and addressed
12. Bases for safety related decisions are documented

SUMMARY OF KEY SAFETY-IN-DESIGN CONCEPTS

- **Establishment and early involvement of integrated project teams (IPTs) and their coordination**
  - Federal and Contractor IPTs; Contractor Safety Design Integration Team (SDIT)
- **Defining the overall strategy for the project, including how safety integration is to be accomplished, and obtaining DOE approval of the strategy**
  - Safety Design Strategy, derived from DOE safety expectations defined in the pre-conceptual phase, is formalized and approved during conceptual design phase

SUMMARY OF KEY SAFETY-IN-DESIGN CONCEPTS

- **Identifying CD-1 as the key point in a project by when major safety systems and design parameters should be defined**
  - Focus on high potential cost safety implications: Hazard Category; building and major components seismic design categories; building confinement strategy; fire protection and power supply system classification
- **Establishing objective criteria for the designation and design of safety structures, systems, and components**
  - STD-1189 Appendices A, B, and C (seismic design basis; collocated worker safety classifications; in-facility worker safety classifications)

SUMMARY OF KEY SAFETY-IN-DESIGN CONCEPTS

- **A conservative front-end approach to safety-in-design that is reflected by a "risk and opportunities" assessment**

  Conservative approach early-on based on assumptions and incomplete information: input to project risk management plan (Risk and Opportunities Assessment) and information for cost estimates

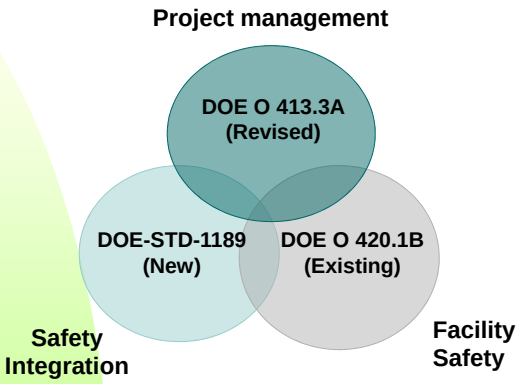
- **Identifying key project interfaces (physical and programmatic) that affect design decisions**

  Project Interfaces: e.g., site infrastructure, security, waste management, emergency preparedness, DNFSB

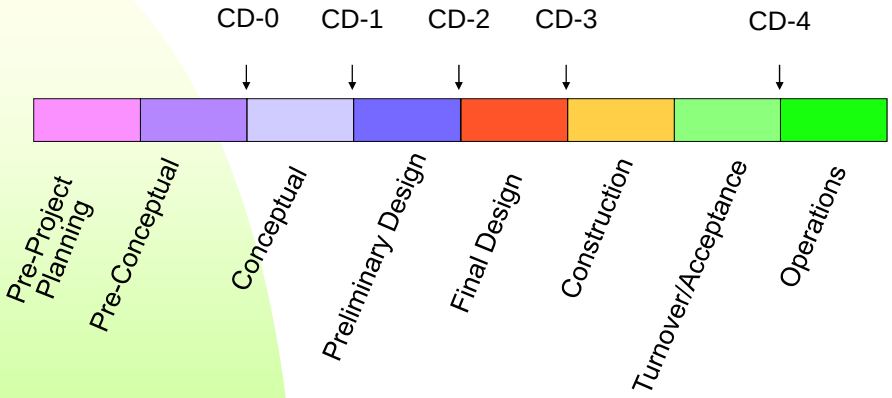
- **Ongoing involvement of regulator(s) in safety-in-design decisions**

  Safety Design Strategy, Conceptual and Preliminary Safety Design Reports, Preliminary Documented Safety Analysis and related DOE reviews and approvals

Project Management with a Safety Focus



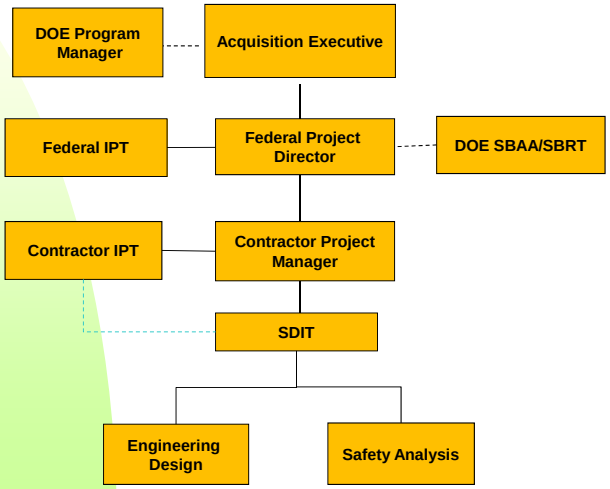
PROJECT LIFECYCLE



KEY COMPONENTS OF PROJECT INTEGRATION AND PLANNING

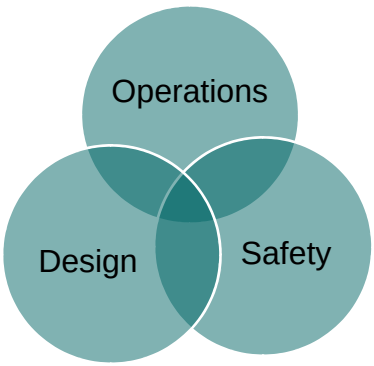
- Federal Project Director
- Federal Integrated Project Team
- Contractor Integrated Project Team
- Safety Design Integration Team

Relationships of Major Project Entities



INTEGRATED PROJECT TEAMS

- Federal Project Director leads an Integrated Project Team (IPT) whose membership should represent the business and technical disciplines necessary for successful execution of the project
- The Federal IPT is the primary tool for breaking down the walls that can exist between different organizations, different professions, and different levels within the different organizations command structures.
- The Contractor IPT is similar to the Federal IPT and is comprised of personnel who ensure integration of mission need, safety analysis, and design
- The SDIT is usually composed of subset of Contractor IPT plus other specialties as needed (Core team: Safety, Design, Operations



Key Actions By Project Phase

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Pre-Conceptual Design Phase

- Prepare a Mission Need Statement
- Identify Potential Hazards, Potential Hazard Classification, and Safety into design **expectations**

Conceptual Design Phase

- Prepare a Safety Design Strategy
- Establish an Integrated Project Team (As soon as possible, no later than CD-1)
- Prepare a Conceptual Safety Design Report
- Prepare a preliminary Project Execution Plan that includes a risk management plan

Key Actions By Project Phase

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Preliminary Design Phase

- Update Safety Design Strategy
- Update Risk Opportunity Assessment
- Prepare Preliminary Safety Design Report

Final Design Phase

- Update Risk and Opportunity Assessment
- Prepare Preliminary Documented Safety Analysis

Key Documents

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Safety Design Strategy (SDS)

- Single source for project safety policies, philosophies, major safety requirements, and safety goals to maintain alignment of safety with the design basis during project evolution.
- Developed from CD-0 definition of DOE expectations for execution of safety during design
- Living document, updated throughout the project stages as needed
- Provides the mechanism by which all elements of the project and approval authorities can agree on basic safety in design approaches
- Prepared by SDIT; reviewed by DOE Safety Basis Review Team (SBRT) ; approved by Federal Project Director and Safety Basis Approval Authority (SBAA)

Key Documents

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Conceptual Safety Design Report (CSDR)

- Documents a preliminary inventory of hazardous materials
- Establishes a preliminary hazard categorization
- Identifies and analyzes facility-level Design Basis Accidents (DBAs)
- Assesses the need for facility-level safety controls (safety SSCs)
- Preliminary assessment of appropriate seismic design bases (facility structure and SSCs)
- Evaluates security hazards that can impact the safety design basis

Conceptual Safety Validation Report (CSVR)

- Prepared by DOE to confirm the preliminary safety positions constitute an appropriately conservative basis to proceed to preliminary design

Key Documents

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Risk and Opportunities Assessment (R&OA)

- Purpose is to recognize and manage risks of proceeding at early stages of design on the basis of incomplete knowledge or assumptions regarding safety issues – input to the overall project Risk Management Plan.
- Risk management strategies must address
  - All technical uncertainties (including schedule and cost implications)
  - Establishment of design margins
  - Increased technical oversight requirements
- SDIT prepares R&OA and updates it throughout the project
- Reviewed by IPT and DOE SBRT and approved by the Federal Project Director (FPD)

Key Documents

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Preliminary Safety Design Report (PSDR)

- Evolves from the CSDR
- Developed to support safety adequacy of the preliminary design effort
- Limited to the extent that design information is also limited
- PSVR prepared by DOE to approve PSDR

Preliminary Documented Safety Analysis (PDSA)

- Evolves from the PSDR
- Completes the analysis of the design
- Format and content covered in Appendix I
  - Based on DOE-STD-3009 format
  - Minimizes need to rewrite for DSA

Experience to Date

- NNSA
- EM
- Other implementation insights?

- BACKUP SLIDES

STD-1189 ROADMAP

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Different parts of the Standard are particularly relevant to different audiences:

For all audiences:

- Preface, with the key concepts and guiding principles upon which the Standard was developed,
- Chapter 1, *Introduction* (background, applicability, must and should) ;
- Chapter 2, *Project Integration and Planning*; and
- Chapter 3, *Safety Considerations for the Design Process*, which provides an overall perspective of the Safety-in-Design process through the Critical Decision stages.

STD-1189 ROADMAP

NUCLEAR EXECUTIVE LEADERSHIP TRAINING

Project safety personnel and DOE safety reviewers

- Chapter 4, *Hazard and Accident Analyses*
- Chapter 5, *Nuclear Safety Design Criteria*
- Chapter 6, *Safety Reports*
- Appendices A through D, dealing with safety SSC and seismic classifications
- Appendix F, *Safety-in Design Relationship with the Risk Management Plan* guides development of the Risk and Opportunities Assessment related to safety assumptions and uncertainties that can affect the project's cost and schedule.
- Appendix G, *Hazards Analysis Table Development* guides this basic safety-in-design input

STD-1189 ROADMAP

- **Project management, both federal and contractor**
  - Chapter 7, *Safety Program and Other Important Project Interfaces*
  - Appendix E, *Safety Design Strategy*
  - Appendix F, *Safety-in-Design Relationship with the Risk Management Plan*
- **Project design personnel**
  - Chapter 5, *Nuclear Safety Design Criteria*,
  - Chapter 7, *Safety Program and Other Important Project Interfaces*,
  - Appendices A through D, which address safety design classifications for safety Structures, Systems, ns Components (SSCs)

STD-1189 ROADMAP

- **Safety Document Preparers and Reviewers**
  - Appendices H and I provide format and content guidance for the preparation of the Conceptual Safety Design Report (CDSA), Preliminary Safety Design Report (PDSA), and Preliminary Documented Safety Analysis (PDSA)
- **Project teams for potential major modifications of existing facilities**
  - Chapter 8, *Additional Safety Integration Considerations for Projects*
  - Appendix J, Major Modification Determination Examples